UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,889	03/22/2004	Eric Henry Grosse	8	1924

7590 07/01/2008

Lucent Technologies Inc.
Docket Administrator (Room 3J-219)
101 Crawfords Corner Road
Holmdel, NJ 07733-3030

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
07/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/805,889
Filing Date: March 22, 2004
Appellant(s): GROSSE, ERIC HENRY

Kenneth M. Brown
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 3/20/2008 appealing from the Office action mailed 10/19/2007.

Art Unit: 2135

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US 2003/0087629	Juitt et al.	5-2003
US 2002/0176579	Deshpande et al.	11-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-7, 12-19, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Juitt et al. (US 2003/0087629)** in view of **Deshpande et al. (US 2002/0176579)**, hereafter "Deshpande".

Considering **Claims 1 and 13,** Juitt discloses a method for establishing a connection from a user terminal to a network through a network access server ([0003] lines 1-3, [0037] lines 1-4, Fig. 1A), the method comprising the steps of: receiving a request from the user terminal to access the network with use of the network access server ([0051] lines 1-7, Fig. 2- step 205); and providing limited network access to the user terminal through the network access server ([0059] lines 1-6, [0068]), wherein providing said limited network access comprises providing network connectivity through said network access server between said user terminal and one or more predetermined enterprise-authenticated hosts ([0059] lines 3-6, [0068] lines 3-6) and not providing network connectivity through said network access server between said user terminal and network sites other than said one or more predetermined enterprise-authenticated hosts ([0068] lines 6-13, [0071] lines 1-3, Fig. 1A- item 117), and wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with each of said one or more known enterprises ([0075] lines 9-12).
Juitt does not explicitly disclose providing limited network access without the user terminal having provided any authentication of an identity thereof to the network access server, and without the user terminal having directly provided any billing or payment information to the network access sever, network access server is

operated by a service provider, wherein said service provider has a pre-existing relationship with each of one or more known enterprises, and wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with each of said one or more known enterprises, and wherein each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises. Deshpande discloses providing limited network access without the user terminal having provided any authentication of an identity thereof to the network access server ([0025] lines 20-24), and without the user terminal having directly provided any billing or payment information to the network access sever ([0025] lines 20-24), network access server is operated by a service provider ([0028] lines 3-5), wherein said service provider has a pre-existing relationship with each of one or more known enterprises ([0028] lines 5-12), and wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with each of said one or more known enterprises [0026] lines 17-21), and wherein each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises ([0028]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Juitt by not requiring any information prior to offering limited access to the network, a service provider having a pre-existing relationship with the enterprise, and a billing service for billing the enterprise as taught by Deshpande. This type of mode will be useful to business employees that need access to a hotspot service provider's services for a business purpose without having to establish an individual subscription with that hotspot service provider (Deshpande- [0028] lines 12-15).

Considering **Claims 2 and 14,** the combination of Juitt and Deshpande discloses the user terminal comprises a wireless device and the network access server comprises a wireless LAN hotspot server (Juitt- Fig. 1A- item 102 and item 120, [0041]).

Considering **Claims 3 and 15,** the combination of Juitt and Deshpande discloses the wireless device and the wireless LAN hotspot server communicate with use of an IEEE 802.11 standard protocol (Juitt- [0038] lines 1-4).

Considering **Claims 4 and 16,** the combination of Juitt and Deshpande discloses request from the user terminal comprises an identification of a given enterprise (Juitt- [0059] lines 1-6, [0071] lines 9-12, Fig. 2- step 210), and wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with said given enterprise (Juitt- [0014], [0075] lines 9-13).

Considering **Claims 5 and 17,** the combination of Juitt and Deshpande discloses user terminal has been pre-configured to automatically provide said identification of the given enterprise (Juitt- [0063] lines 1-7).

Considering **Claims 6 and 18,** the combination of Juitt and Deshpande discloses request from the user terminal further comprises a fixed password, said fixed password uniquely associated with said given enterprise (Juitt- [0059] lines 13-18).

Considering **Claims 7 and 19,** the combination of Juitt and Deshpande discloses user terminal has been pre-configured to automatically provide said identification of the given enterprise and said fixed password (Juitt- [0063] lines 1-7).

Considering **Claims 12 and 24,** the combination of Juitt and Deshpande discloses the step of providing said limited network access comprises the steps of: comparing a first IP address pair to a set of previously stored IP address pairs, the first IP address pair comprising an IP address of said user terminal and an IP address of an intended destination to which access has been requested by said user terminal, and each IP address pair in

the set of previously stored IP address pairs comprising the IP address of a user terminal connected to said network access server and an IP address of one of said one or more enterprise-authenticated hosts; and providing network connectivity between said user terminal and said intended destination if and only if said first IP address pair matches one of said IP address pairs in said set of previously stored IP address pairs (Juitt- [0073] lines 7-14, Deshpande- [0026] lines 5-16). Applicant also discloses that this technique is one that is well known in the art (Applicant Admitted Prior Art- AAPA [Grosse] - p. 21- lines 9-21, p. 22- lines 1-2).

(10) Response to Argument

Juitt et al. in view of Deshpande.

Group #1: **Claims 1-7, 12-19, and 24.**

Appellant argues that the combination of Juitt and Deshpande fails to teach "providing limited network access without the user terminal having provided any authentication of an identity thereof to the network access server…and without the user terminal having directly provided any billing or payment information to the access server." Juitt – [0059] discloses that during authentication, all requests from the mobile device are redirected to the authentication web page such as authentication to an enterprise-authenticated host, therefore supplying the mobile user with limited network access. Access is limited in the sense that the mobile user is connected to the network and limited to accessing only the authentication webpage. The exact citation from Juitt – [0059] is disclosed below:

> "[0059] In one embodiment, authentication (STEP 210) is accomplished by interaction with an authentication web page maintained by, for example, the authentication server 125. The local gateway server 120 redirects all requests from the mobile device 100 made with a particular protocol (e.g., HTTP) to the authentication web page. The mobile device 100 (or the user of the mobile device 100) then supplies identifier and authentication information to the authentication web page. Identifier information can include one or a combination of a username, e-mail address, or other unique name associated with the user of the mobile device 100, the mobile device 100, an object such as a smart card, and so on. Authentication information can include one or a combination of personal identification number (PIN), password, encryption key, biometric information, digital certification, and digital code, as

> well as other information that is associated with at least one of the user of the mobile device 100, the mobile device 100, a smart card, and so on."

Therefore, Juitt explicitly discloses providing limited network access to the user terminal through the network access server (i.e. accessing an authentication webpage upon connecting to the network).

Deshpande – [0025] lines 20-24 discloses that certain users are able to connect to the wireless hotspot within the hotel, coffee shop, or airport without identification and/or authentication services. The exact citation from Deshpande is disclosed below:

> "Further, certain users/devices may be able to connect with and request or accept services from the hotspot service provider network without identification and/or authentication such as no-charge Internet access or location-based services supported by advertisements."

Therefore, when taken in combination, the combination of Juitt and Deshpande teaches providing limited network access (i.e. accessing an authentication webpage upon connecting to the network) without the user terminal having provided any authentication of an identity thereof to the network access server (i.e. connect to the provider network without identification/and or authentication).

With respect to appellants' argument that the combination fails to teach "and without the user terminal having directly provided any billing or payment information to the network access server." Deshpande – [0028] discloses operating in 3 modes (business, public, and personal). In business mode, a business entity (i.e. enterprise) is billed for the use of services from the hotspot service provider network. This type of billing requires a pre-existing relationship between the hotspot service provider and the business entity to be charged. Specifically, Deshpande – [0028] discloses:

> "business arrangements are needed between the hotspot service provider network and the business entity such as direct arrangements where a business subscription with the hotspot service provider has been provided for the user/device…is used for business purposes and such usage is billed to a business entity."

Therefore, Deshpande explicitly discloses without the user terminal having directly provided any billing or payment information to the network access server (i.e. previous business arrangements).

Appellant argues that Deshpande only discloses "access to free hotspot service provider services." However, when taking in combination with Juitt, the combination teaches for example, walking into an airport and requesting a connection to the network. This request is granted and the user receives limited access to the network in that they only have access to the authentication webpage (i.e. the enterprise-authenticated host webpage). This has all been accomplished without the user supplying any authentication information to the hotspot service provider. Usage charges are billed to the business entity/enterprise through previously made "business arrangements."

Appellant argues that the combination fails to teach "said service provider has a pre-existing relationship with each of one or more known enterprises...and wherein each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises." As previously discussed, Deshpande – [0028] discloses pre-existing "business arrangements" used to bill the business entity/enterprise for charges incurred by the user. Deshpande goes on to provide motivation for the arrangements in that individual users (i.e. employees) will not have to set up individual subscriptions with each hotspot service provider. Deshpande – [0028]:

> [0028] In an embodiment, three modes are provided: a business or private mode, a public mode and a personal mode. In the business or private mode, a business entity is billed for user/device usage of services from a hotspot service provider network. In this mode, business arrangements are needed between the hotspot service provider network and the business entity such as direct arrangements where a business subscription with the hotspot service provider has been provided for the user/device or indirect arrangements where a personal user subscription is used for business purposes and such usage is billed to a business entity. This type of mode will be useful to business employees that need access to a hotspot service provider's services for a business purpose without having to establish an individual subscription with that hotspot service provider.

Therefore, the combination of Juitt and Deshpande discloses said service provider has a pre-existing relationship with each one of one or more known enterprises (i.e. previous business arrangements)…and wherein each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal (i.e. access to the authentication webpage) incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises (i.e. billed to a business entity).

Appellant argues that Deshpande grants and incurs charges on full access to the hotspot. The combination of Juitt and Deshpande discloses that businesses incur charges for limited access (i.e. authentication webpage) to the hotspot service provider network. Deshpande – [0025] lines 20-24 discloses limited access to the network without identification:

> "Further, certain users/devices may be able to connect with and request or accept services from the hotspot service provider network without identification and/or authentication such as no-charge Internet access or location-based services supported by advertisements."

In combination with Juitt- [0059], this limited access limits users to an authentication enterprise authenticated host webpage:

> "[0059] In one embodiment, authentication (STEP 210) is accomplished by interaction with an authentication web page maintained by, for example, the authentication server 125. The local gateway server 120 redirects all requests from the mobile device 100 made with a particular protocol (e.g., HTTP) to the authentication web page.

Therefore, charges incurred by the business entity are for the limited network access provided to the user, not for full access to the hotspot service provider network. As previously discussed, these charges are then billed to the business entity through pre-existing business arrangements.

Appellant argues that "business or private mode access not only requires authentication, but employs high encryption…to essentially create a virtual private network (VPN) and that would be most useful to business or individual users/devices requiring high security (e.g. accessing a corporate LAN)." Appellants own claims require "wherein said request from the user terminal comprises an identification of a given enterprise,

and wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with said given enterprise (Claim 4 of the Instant Application). The combination of Juitt and Deshpande utilizes the VPN in the same manner as the instant application (i.e. for authentication to the enterprise after limited access is granted by the hotspots). From the combination of Juitt and Deshpande, it is clearly seen that no authentication (i.e. accept services without identification/authentication, Deshpande- [0025]) is required to gain limited access to the network (i.e. authentication/enterprise-authenticated host webpage, Juitt- [0059]). Followed by the user authenticating themselves to the VPN gateway corresponding to a business entity/enterprise (i.e. high encryption is used to create a VPN, Deshpande- [0026]). This is the same process claimed in the application as can be seen in Claim 1 and Figs. 5-6 of the instant application.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/R. D. M./

Examiner, Art Unit 2135

Art Unit: 2135

Conferees:

/HOSUK SONG/

Primary Examiner, Art Unit 2135

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135